

Developing Security Controls for OT

**Information Security forum for Texas
Government**



‘Who am I? Why am I here?’

**To tell a cybersecurity
success story ...**



**... and a business success
story**



Spoiler alert!

- **LCRA's unique mission**
- **The technology and organizational background**
- **A challenging audit that presented an exciting opportunity**
- **How we responded**
- **How it was received**
- **How it was implemented**
- **Lessons learned**

‘So, what is it y’all do at LCRA?’

Energy?

Water?

Community Service?

Yes!

Our mission:

To enhance the quality of life of the Texans we serve through water stewardship, energy and community service.

Setting up (the cyber) shop

- 2014 – new executive leadership at LCRA and the creation of a 4-person Cybersecurity department
- LCRA leadership commitment to cybersecurity and providing resources
- NIST 800-53
- The emergence of nation-state threat actors
- Critical infrastructure as a target
- Blurring lines between physical and digital security



All the precedence men

- Policies not consistent
- Policies not effectively communicated
- Cybersecurity department's authority not clearly defined
- “No clear order of precedence” for the standards that are to be followed

‘Management has become aware ...’

- **Convene a cross-functional team**
- **Identify overlapping standards**
- **Determine order of precedence**
- **Create policies that account for the differences in IT and OT**
- **Define roles and responsibilities**
- **Communicate and train**
- **Deadline of Oct. 31, 2019**

‘How are we going to get that done?’

- **Get the stakeholders involved**
- **Identify the external standards and map them to current controls**
- **Draft security controls specifically for the ICS environment**
- **Draft a document explaining LCRA’s cybersecurity program**
- **Get approval from stakeholders**

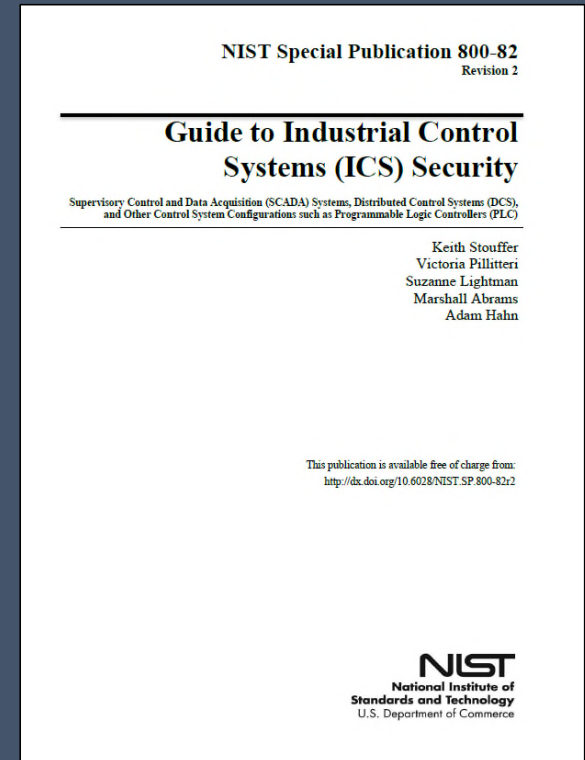
Time to pop the question

- CISO convened a cross-functional team meeting with more than 20 people from across the organization
- Reviewed the audit findings and management response
- Followed up with individual meetings
- Defined and answered two key questions:
 - How do we organize/categorize systems?
 - What external standards should we include in the controls?



Standard objections

- NIST 800-82, Guide to Industrial Control Systems Security
- International Society for Automation (ISA), Security for industrial automation and control systems
- Institute of Electrical and Electronics Engineers (IEEE) – Standard for Intelligent Electronic Devices Cyber Security Capabilities
- NERC CIP



‘You’ve been drafted’

- **Two members of the Cybersecurity department were given responsibility for drafting the ICS controls**
- **Worked through the wording of each control to create the default control language**
- **Included compensating controls**
- **Inserted the external controls**
- **Consulted SMEs as appropriate**

‘But what’s it going to look like?’

- **Content needed to be professional and user friendly**
- **Include the default controls and external controls**
- **Available in multiple formats**
- **Provide clear guidance for use**
- **The LCRA Cybersecurity Framework**

5.0 How to Read and Use This Document

1

Ctrl No.	Name
AC-7	Unsuccessful Logon Attempts

2

LCRA Control

Accounts on LCRA ICS shall have controls in place [REDACTED]. These events will generate an alert to the cybersecurity coordinator and cybersecurity department. The locked out account shall [REDACTED] until [REDACTED] unlocks the account.

3

Compensating Control:

- In instances where ICS must remain continuously on and operators remain logged onto the system at all times, a "log-over" capability may be employed. Compensating controls include logging or recording all unsuccessful login attempts and alerting identified facility security personnel through alarms or other means when the number of LCRA defined consecutive invalid access attempts is exceeded.

4

Related Controls

ISA

ISA 62443-2-1:2009 4.3.3.6.4: Log files should record all access attempts to critical systems and should be reviewed for successful and failed access attempts.

IEEE

None

NERC CIP

CIP-007-6 R4.1: Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

- 4.1.1. Detected successful login attempts;
- 4.1.2. Detected failed access attempts and failed login attempts;
- 4.1.3. Detected malicious code.

CIP-007-6 R5.7: Where technically feasible, either:

- Limit the number of unsuccessful authentication attempts; or
- Generate alerts after a threshold of unsuccessful authentication attempts.

1

Control Number and Name: This section references the security control number and name defined in the applicable National Institute of Standards (NIST) 800-82 publication.

2

LCRA Control: This is the default cybersecurity control for ICS at LCRA. If the business unit or department does not use a separate standard, like ISA or IEEE, this control applies.

3

Compensating Control: In some instances, compliance with a control is not possible for business reasons or because of characteristics of the ICS. In those cases, a compensating control may be applied which helps mitigate risk.

4

Related Control: This section includes controls and requirements from ISA, IEEE and NERC CIP that correspond to the subject matter contained in the LCRA Control. Departments that use ISA and IEEE instead of the LCRA Control can find the applicable controls here. NERC CIP requirements are provided here as a reference to show their relationship to LCRA's cybersecurity controls. This information should not be used as objective evidence for NERC CIP compliance.

‘You brought us a Rolls Royce!’

- Our work product was circulated internally for approval
- Sent out to key stakeholders from the cross-functional team for review
- Followed up with individual meetings – met with enthusiastic approval
- Presented to top executives for sign off






Now what?

- Risk Management team leads CSF Assessments of individual business units and systems
- Collaborative process throughout
- LCRA CSF Self-Scoring tool – answers identify areas of strength and notable gaps
- Leadership from both groups establishes target tier

<div><div>Tier 1</div><div>Tier 2</div><div>Tier 3</div><div>Tier 4</div></div>							
<div><div>Tier 1: Partial<ul style="list-style-type: none">Not formalizedAd hocLimited awarenessLimited external coordination</div><div>Tier 2: Risk-Informed<ul style="list-style-type: none">Approved but not establishedNot consistent across the organizationInformal</div><div>Tier 3: Repeatable<ul style="list-style-type: none">Formal risk managementOrganizationally consistentRespond to risk changesCollaborate with external parties</div><div>Tier 4: Adaptive<ul style="list-style-type: none">Improve based on lessons and indicatorsRisk management is part of cultureActive information sharing with external parties to drive action</div></div>							
Response Planning		Policy Score	Practice Score	Tier	Control	Policy	LCRA Controls Mapping
RS.RP-1: Response plan is executed during or after an incident	RS.RP-1	3	3	Repeatable	<div>CP-2 Develop and maintain contingency plans for ICS.</div> <div>CP-10 Employ processes and controls to ensure it is possible, after a compromise, disruption or failure of an ICS, to recover and reconstitute the ICS to a previously known state. The processes and controls must take into account whether restoration procedures may disrupt ongoing physical processes or adversely affect</div>	Incident Response Policy and Procedures	CP-2, CP-10, IR-4, IR-8

Profile Assessments & System Security Profile

- CSF Profile Assessment – identifies opportunities for improving cybersecurity
- System Security Profile (SSP) – provides controls that are either in place or that are to be implemented to meet target goal
- SSP is used to re-evaluate maturity level a year after assessment.

Categories and subcategories			
Meets target tier  Below target tier  Scored at organization level 			
Asset Management	Current Tier	Target Tier	Required Actions or Mitigations
ID.AM-1: Physical devices and systems within the organization are inventoried	3	4	- Review and update policy and procedure for inventorying physical devices and systems.

DETECT	Anomalies and Events: Anomalous activity is detected and the potential impact of events is understood.	<ul style="list-style-type: none"> A visual diagram for expected <SYSTEM> data flow is created and maintained All <SYSTEM> systems should participate in and report to the SIEM
	Security Continuous Monitoring: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	<ul style="list-style-type: none"> Malicious code detection software is installed on all systems External service provider activity related to <SYSTEM> is monitored to detect potential cybersecurity events

CYBERSECURITY FRAMEWORK

- Framework +
- Getting Started +
- Perspectives +
- Frequently Asked Questions +
- Events and Presentations +
- Informative References +
- Resources +
- Newsroom +
- Related Programs
- Cybersecurity @ NIST

CONNECT WITH US



Success Story: Lower Colorado River Authority

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.



"As a critical infrastructure provider, LCRA faces the full spectrum of cyber threats. LCRA's adoption of the NIST Cybersecurity Framework enables risk-based business decisions that protect our dams, power plants, electric transmission and telecommunication systems. Successfully securing such diverse businesses requires flexibility and adaptation. The Cybersecurity Framework is the core means for LCRA to establish business objectives, assess risk and establish appropriate security controls." – Madhava Utigikar, LCRA CISO

‘The friends we made along the way’

- **Audits can be opportunities**
- **Resources aren’t enough and relationships are essential**
- **People do care about cybersecurity**
- **Make your customers part of your governance development process – you want their expertise and buy in**
- **The challenges that scare you the most are often easier to resolve than you think**
- **Act in good faith, show you’re making an effort**
- **Set your project up for success once it’s done**